ABSTRACT OF THE DISCLOSURE

An equation transforming unit triangular transforms a matrix M and a vector v to generate a matrix M' and a vector v' for a system of linear equations $M'x=v'$ in n unknowns that has an equivalence relation with a system of linear equations $Mx=v$ in n unknowns. The triangular transformation is such that the matrix M is transformed into an upper triangular matrix without the diagonal elements of the matrix M being changed to 1. An inverting unit calculates the inverses of the diagonal elements of the matrix M'. An equation computing unit finds the solutions of the system of linear equations $M'x=v'$ using the matrix M', the vector v', and the calculated inverses of the diagonal elements. An inverse computing unit computes the inverse I of an element y in $GF(q)$ which is an extension field of a finite field $GF(p)$, based on the solutions found by the equation computing unit.